Mini-Challenge 3

Supplementary Data Descriptions for Week 2 Data

Data Sources

You have five sources of data and information at your disposal in order to characterize what is happening on the network in Week 2 of the scenario:

1. A network description and network diagram reflecting the configuration used for Week 2. This is described below.
2. Intrusion protection system (IPS) data for the network. This data is described below.
3. Network flow data (netflow data). This data format is unchanged from Week 1. It is described in the file "Week 1 Data Descriptions final.pdf".
4. Network health and status data (Big Brother data). This data format is unchanged from Week 1. It is described in the file "Week 1 Data Descriptions final.pdf".
5. Questions to the Big Marketing corporate office. This is described on the VAST Challenge MC3 web site.

1. Network Description

Organizationally, Big Marketing consists of three different branches, each with around 400 employees and its own web servers. The Big Marketing network diagram was updated for Week 2 to reflect the addition of an intrusion protection system (IPS). The revised network diagram is shown in the "VAST Challenge 2013 Network Architecture Week 2.PDF" file. The detailed list of IPs and their mapping to hostnames is included in the file BigMktNetwork.txt, which was provided with the Week 1 data.

All Big Marketing workstations and servers sit behind a firewall, including the web servers that the company operates for their clients. The customers of Big Marketing's clients visit theses web servers regularly.

The Big Marketing network uses network address translation (NAT). External visitors to the Big Marketing network use one set of external IP addresses to access the Big Marketing web sites, but as they enter the Big Marketing network, they get translated into a second set of internal IP addresses.

The following table shows the mapping of NATed IP addresses for servers that are accessible outside the company firewall.

Table 1. IP Address Cross-Reference

Server Name	Internal IP address	External IP address
DC01.BIGMKT1.COM (DNS)	172.10.0.2	10.0.2.2
EMAIL01.BIGMKT1.COM	172.10.0.3	10.0.2.3
WEB01.BIGMKT1.COM	172.10.0.4	10.0.2.4
WEB01A.BIGMKT1.COM	172.10.0.5	10.0.2.5
WEB01B.BIGMKT1.COM	172.10.0.7	10.0.2.6
WEB01C.BIGMKT1.COM	172.10.0.8	10.0.2.7
WEB01D.BIGMKT1.COM	172.10.0.9	10.0.2.8
DC02.BIGMKT2.COM (DNS)	172.20.0.2	10.0.3.2
EMAIL02.BIGMKT2.COM	172.20.0.3	10.0.3.3
WEB02.BIGMKT2.COM	172.20.0.4	10.0.3.4
WEB02A.BIGMKT2.COM	172.20.0.5	10.0.3.5
WEB02B.BIGMKT2.COM	172.20.0.6	10.0.3.6
WEB02C.BIGMKT2.COM	172.20.0.7	10.0.3.7
WEB02D.BIGMKT2.COM	172.20.0.8	10.0.3.8
WEB02L.BIGMKT2.COM	172.20.0.15	10.0.3.15
DC03.BIGMKT3.COM (DNS)	172.30.0.2	10.0.4.2
EMAIL03.BIGMKT3.COM	172.30.0.3	10.0.4.3
WEB03.BIGMKT3.COM	172.30.0.4	10.0.4.4
WEB03A.BIGMKT3.COM	172.30.0.5	10.0.4.5
WEB03B.BIGMKT3.COM	172.30.0.6	10.0.4.6
WEB03C.BIGMKT3.COM	172.30.0.7	10.0.4.7
WEB03D.BIGMKT3.COM	172.30.0.8	10.0.4.8

2. Intrusion Protection System Data

An intrusion protection system (IPS) monitors and logs network activities. When it identifies apparently malicious activity, the IPS attempts to block or prevent the activity. In this case, Big Marketing used Cisco Adaptive Security Appliance model ASA5510 with Threat Detection Mechanisms enabled. The IPS was configured with default detection rules as well as specialized, site-specific rules.

The resulting log messages were run through a parser and loaded into a table. They are being released comma-separated values (.csv) files.

The following table describes the fields in the IPS log table.

Table 2. IPS Log Fields

Field Name	Field Type	Field Description	Field Explanation
dateTime	varchar	Date and time in the format <dd/Mon/yyyy hh:mm:ss>	The date and time on which the message was logged
priority	varchar	Message priority	The priority of the message. Potential values, ranging from most to least severe: • Alert • Critical • Error • Warning • Notice - Notification • Info - Informational • Debugging
operation	varchar	Operation	A term describing the operation being logged. Examples: • Built • Teardown • Deny
messageCode	varchar	Message code, in the format <ASA-n-nnnnnn>	The message code associated with this message. The first three letters are 'ASA', followed by a number corresponding to the message priority, and finally the specific message number. The full list of message codes can be found at http://www.cisco.com/en/US/docs/security/asa/asa82/system/message/logmsgs.html or in http://www.cisco.com/en/US/docs/security/asa/asa80/system/message/logmsgs.pdf. Common message codes are described in Table 3.
protocol	varchar	IP Layer protocol	The textual form of the IP layer protocol. Examples: TCP, UDP.
srcIp	varchar	Source IP address <aaa.bbb.ccc.ddd>	Source IP address.

destIp	varchar	Destination IP address <aaa.bbb.ccc.ddd>	Destination IP address.
srcPort	varchar	Source Port	Source ports for TCP and UDP protocol transactions.
destPort	varchar	Destination Port	Destination ports for TCP and UDP protocol transactions.
destService	varchar	Destination Service	Destination service for the traffic
direction	varchar	Direction	Direction of the flow. Values: Inbound, Outbound, (empty)
flags	varchar	Flags	Flags that provide additional information in specific messages. Not all messages have flags, and flag values vary by message type. Example values: ACK, Connection timeout.
command	varchar	Command	This field is not used in this scenario

A sample of the IPS data has been pulled into Microsoft Excel and shown below.

dateTime	priority	operation	messageCode	protocol	SrcIp	destIp	srcPort	destPort	destService	direction	flags	command
4/10/2013 7:02	Info	Built	ASA-6-302013	TCP	172.10.2.35	10.1.0.75	2507	80	http	outbound	(empty)	(empty)
4/10/2013 7:02	Info	Teardown	ASA-6-302014	TCP	172.30.1.104	10.0.0.14	2651	80	http	outbound	TCP FINs	(empty)

The list of common message codes appears in the table below.

Table 3. Common IPS Message Codes

Message Code	Text
ASA-4-106023	Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID [0x8ed66b60, 0xf8852875]
ASA-6-106015	Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name.
ASA-6-302013	Built {inbound|outbound} TCP connection_id for interface:real-address/real-port (mapped-address/mapped-port) to interface:real-address/real-port (mapped-address/mapped-port) [(user)]
ASA-6-302014	Teardown TCP connection id for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [reason] [(user)]
ASA-6-302015	Built {inbound|outbound} UDP connection number for interface_name:real_address/real_port (mapped_address/mapped_port) to interface_name:real_address/real_port (mapped_address/mapped_port) [(user)]
ASA-6-302016	Teardown UDP connection number for interface:real-address/real-port to interface:real-address/real-port duration hh:mm:ss bytes bytes [(user)]